1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld Bureau of Administration Global Information Services Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: June 7, 2012

(b) Name of systems: electronic Document Processing, electronic Document Processing Web report (child to eDP)

(c) System acronyms: eDP, eDP Web

(d) IT Asset Baseline (ITAB) numbers: 5091, 5092

(e) System description (Briefly describe scope, purpose, and major functions):

electronic Document Processing (eDP) is a smart-client Windows application that is installed on National Visa Center (NVC) workstations that allows its users to scan, attach, view, edit, or delete support documentation received at NVC for immigrant visa (IV) cases. eDP mission requirements, in support of the Bureau of Consular Affairs, are to:

- Provide an interface for National Visa Center (NVC) staff to upload the electronically received immigrant visa supporting documentation and store it to the Consular Consolidated Database (CCD) so that it is viewable by post
- Provide an interface to scan the paper files received at NVC and store them electronically

Possible IV case types include:

- Adoption
- Amerasian Immigrants
- Battered Spouse/ Child
- Employment
- Family
- Fiance K1
- Parole
- Special Immigrant Visa (SIV)
- Spouse K3
- Widow/ Widower

The eDP application communicates with its database to store data that it scans from paper files or uploads from electronic files (including binary or bin files). The electronic document data stored in the database will be replicated to the CCD whenever there are inserts or updates to document records. Once the documents are in the CCD, they are accessible to users at Posts on the OpenNet via the electronic Document Processing web report (eDP Web).

eDP Web is the web component used by all the posts and external agencies such as the Department of Homeland Security (DHS) to view the immigrant visa (IV) documents related to IV cases. The eDP Web user is able to perform searches to retrieve and view all documents associated to a case or an applicant in a printable report format. eDP Web is available as a menu item in a CCD report. The IV documents are viewed from eDP Web via a web service call to CCD.

(f) Reason for performing PIA:

- ☒ New system
- ☐ Significant modification to an existing system
- ☐ To update existing PIA for a triennial security reauthorization

(g) Explanation of modification (if applicable): N/A

(h) Date of previous PIA (if applicable): N/A

3. Characterization of the Information

The system:

- ☐ does NOT contain PII. If this is the case, you must only complete Section 13.
- ☒ does contain PII. If this is the case, you must complete the entire template.

The eDP primarily collects and maintains information on foreign nationals as part of the U.S. immigrant visa (IV) application process. As such, the information provided by the IV applicant is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA). Because the visa applicants themselves are not U.S. persons (that is, U.S. citizens or legal permanent residents), they are not covered by the provisions of the E-Government Act of 2002, OMB 03-22, and Privacy Act of 1974.

However, an IV application may include personally identifiable information (PII) about persons associated with the immigrant visa applicant who are U.S. citizens or legal permanent residents.

This PII on U.S. persons may include the following: U.S. sponsor's name, address and phone number; U.S. contact name, address and phone numbers; and employer name, address and phone numbers; legal representative name, address, and phone numbers. The source of information is the visa applicant, petitions, and visa applications.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

The data elements of foreign nationals collected by eDP for IV cases are obtained directly from the Immigrant Visa (IV) applicant or petitioner (family member submitting the application on behalf of the applicant), or legal representative when he/she submits supporting documentation (e.g. birth certificate, marriage certificate, biographical data

form, resettlement application, passport) for the applicant's IV case. Those data elements are as follows:

The elements of PII that are collected by eDP and maintained in eDP Web are

- Passport Number (foreign)
- Last name
- First and Middle names
- Date of Birth
- Home address
- Home telephone number
- Business telephone number
- Mobile/cell telephone number
- Email Address
- Passport Issuance (City, Country, State/Province)
- Passport Issuing Country
- Passport Date of Issuance
- Passport Expiration Date
- Alias (Other) Names
- Place of Birth (City, Country, State/Province)
- Nationality
- Gender
- National ID (if applicable)
- Marital Status
- Spouse's Full Name
- Spouse's DOB
- Child's Full Name
- Child's DOB
- Name & Address of present Employer or School
- Occupation
- Address (in US)
- Name & Telephone Number of point of contact in US

b. How is the information collected?

Information is submitted to the NVC via forms and documents mailed by the IV applicant, petitioner or legal representative. Documents are scanned or uploaded into eDP via an eDP client workstation application. Once collected via eDP, the information can be viewed via eDP Web.

The following forms collected via eDP may contain PII:

DS-0234	Special Immigrant Visa Biodata Form
DS-157	Supplemental NIV Application
DS-230	Immigrant Visa Application
I-797	Notice of Action
I-864	Affidavit of Support
I-864A	Household Member Affidavit of Support

I-864EZ	EZ Affidavit of Support
I-864W	Affidavit of Support Exemption Form
I-130	Petition for Family Relative
I-800	Petition for Convention Adoptee
I-526	Petition by Entrepreneur
I-129F	Petition for Alien Fiance/Spouse
I-600	Petition for Orphan
I-730	Petition for Refugee/Asylee Relative
I-360	Petition for Amerasian, Widow(er), or Special Immigrant
I-929	Petition for U-1 Relative
I-140	Immigrant Petition for Alien Worker
I-600A	Petition for Orphan/Advance Processing
I-824	Application for Action on Approved Application or Petition

c. Why is the information collected and maintained?

The information is collected for the purpose of substantiating the statements made on the immigrant visa application. Information is collected to perform background checks of IV applicants in support of issuance processing and document verification in order to identify individuals who are ineligible for an IV or who require special action. Documentation uploaded at NVC is replicated to CCD to provide electronic attachments for the applications under consideration.

d. How will the information be checked for accuracy?

After documents are scanned into eDP quality assurance is performed to ensure that those documents were scanned in correctly. Once documentation is viewable in eDP Web, an accuracy check is performed. After comparing and verifying the electronic documents against the originals obtained during the post interview, an eDP Web user at post who is designated as an Immigrant Visa Overseas Foreign Service Officer (IVO FSO) then marks the electronic document as “Original Seen and Compared”. This is the only type of user in eDP Web who is able to mark documents. Accuracy is the responsibility of the IV applicant. Any errors or omissions detected during the IV application review process are called to the attention of the applicant.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

eDP and eDP Web were developed and modified to support U.S. immigration and nationality law as defined in the major legislation listed below:

- Immigration and Nationality Act (INA) of 1952, 8 U.S.C. 1101, et al. (as amended)

- INA, 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- INA, 8 U.S.C. 1202(f) (Confidential Nature of Visa Records)
- 22 U.S.C 2651(a) (Organization of Department of State)
- Immigration Act of 1990 (P.L. 101-649)
- Illegal Immigration Reform and Immigration Responsibility Act of 1996 (IIRIRA) (P.L. 104-208)
- Omnibus Consolidated Appropriations Act, 1997 (P.L. 104-208)
- Legal Immigration Family Equity "LIFE" Act (Part of HR 5548, 2000)
- USA PATRIOT Act of 2001 (P. L. 107-56)
- Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173)
- Child Status Protection Act of 2002 (P.L. 107-208)
- Anti-Drug Abuse Act of 1988 (P.L. 100-690)

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The personal data collected by eDP is the minimum necessary to carry out the function of eDP/eDP Web as identified in Section 3(c) above.

Due to the strict security controls required by all Department of State systems before system operation commences, privacy risks are generally limited to three categories. The most common ways in which PII can become exposed to unauthorized users and potentially vulnerable to identity theft are:

- **Device theft or loss** Lost or stolen laptops and other devices such as removable drives may contain PII.

- **Portable Devices** PII is at the fingertips of every staff member who has email, database and Web access at work. The growing use of removable media such as USB drives, CDs/DVDs and portable Mp3 players creates risk by making PII easily transportable on devices that aren't always properly secured.

- **Insider threat** Disgruntled employees seeking revenge or inadvertent human error to send PII over the internet.

The consequences to organizations or individuals whose PII has been exposed to unauthorized users may include the following:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss
- Harm to Department programs or the public interest
- Unauthorized release of sensitive information
- Threats to personal safety
- Civil or criminal violation

In accordance with the Federal Information Security Management Act of 2002 (FISMA) and the information assurance standards published by the National Institute of Standards and Technology (NIST), management, operational, and technical security controls are implemented to protect the data. These controls include regular security assessments, physical and environmental protection, encryption, access control,

personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software), training, and audit reports.

4. Uses of the Information

a. Describe all uses of the information.

The information collected by eDP is used for processing, auditing, and tracking of individual immigration visa applications. The documents scanned into eDP provide electronic versions of the required documents needed to determine IV eligibility by substantiating information entered by the applicant. These required documents are necessary to complete the applications that are held in the Immigrant Visa Information System (IVIS), the system used to manage the processing of immigrant visa petitions.

b. What types of methods are used to analyze the data? What new information may be produced?

eDP users do not analyze the data. They only perform quality assurance on the scanned forms to ensure that they were scanned correctly. eDP Web users can perform searches on the data to find a particular IV case or applicant. Upon selecting one of the applicant names returned in the search results, the eDP Web user can then select one of the applicants to view the list of documents attached to that applicant. The allowed transactions are to view, save, print the documents, and in the case of the IVO FSO, to mark the document as “Original Seen and Compared”. No data mining is performed and no new information is produced.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

IV applicant data such as photos, fingerprints, drivers’ licenses, birth place records, military service, or existing passports are provided by IV applicants and/or foreign authorities. The publicly available information or information from other Federal agency databases such as birth certicates, adoption papers, tax returns and military records is provided by the applicant or petitioner in order to effectively identify the IV applicant and to complete the application process.

d. Are contractors involved in the uses of the PII?

eDP is a government owned system. Government personnel are the primary users of eDP; however, contractors are involved with the design, development and maintenance of the system. Privacy Act information clauses have been inserted into all Statements of Work and become part of the signed contract. All users are required to pass annual computer security/privacy training, and to sign non-disclosure and rules of behavior agreements. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

eDP scanning can only be done at the NVC facility using a government-owned workstation. User access to information is restricted according to job responsibilities and requires managerial level approvals. Access control lists permit categories of

information and reports that are to be restricted. Roles determine what a user can do within eDP and eDP Web. Security Officers determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance. Mandatory annual security/privacy training is required for all authorized users including security training and regular refreshment training.

All users are screened prior to their employment with the Department of State or with their respective agency. The Bureau of Diplomatic Security is responsible for the investigations of personnel in conjunction with normal hiring practices. This investigation consists of a review of a completed security questionnaire, a name check against applicable government, police, credit and fingerprint records, and may include a personal interview if warranted. In addition, before they are given access to the OpenNet and any CA/CST system, including eDP/ eDP Web, users are required to sign non-disclosure agreements, acceptable use agreements, conflict-of-interest agreements, and rules of behavior agreements.

Contractors who support eDP/ eDP Web are subject to a rigorous background investigation by the contract employer and are checked against several government and criminal law enforcement databases for facts that may bear on the loyalty and trustworthiness of the individual. At the very minimum, contractors involved in the development and/or maintenance of eDP/ eDP Web hardware and software must have a level "Secret" security clearance. Once the highest-level background investigation required has been completed, cleared technical personnel (government and contractors) will be allowed to access the server rooms housing eDP/ eDP Web. Consular post officers/users, system administrators, and database administrators are trained through the security awareness training to safeguard PII from unauthorized users by storing diskettes, CDs, and printouts in a safe and secure manner. Shredders and/or burn boxes are provided throughout the post and domestic sites for the proper disposal of paper that contains PII.

5. Retention

a. How long is information retained?

The retention time of the visa records is specified in the U.S. Department of State Records Disposition Schedule, Chapter 14: Visa Records and varies depending upon the specific kind of record and whether or not a visa was issued. If the applicant was refused a visa, the period of retention depends on which sections of the Immigration and Nationality Act the ruling of ineligibility was based on. Files of closed cases are retired or destroyed in accordance to the published record schedules of the Department of State and the National Archives and Records Administration. Some records, such as refused records, are retained until the subject is 100 years old and 10 years have passed since the last visa activity. Procedures are documented at the Office of Freedom of Information, Privacy, and Classification Review, Room 1239, Department of State, 2201 C Street NW, Washington, DC 20520-1239.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

Records retention bears on privacy risk in two ways. First, the longer the records exist, the greater they are at risk to unauthorized use or exposure. Second, the longer records exist, the more likely inaccuracies will develop as a consequence of aging. The privacy risks are mitigated through the controlled access and rules of behavior that govern the uses of eDP/ eDP Web throughout the lifetime of the data. The information is only retained for the amount of time that is required to perform the system's purpose.

All physical records containing PII are maintained in secured file cabinets or in restricted areas, to which access is limited to authorized personnel. Access to computerized files is password-protected and under the direct supervision of the system manager. When records have reached their retention end-date, they are immediately retired or destroyed in accordance with the National Archive and Records Administration (NARA) rules.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

Consular Consolidated Database (CCD) – CCD connects to eDP so that IV supporting documents (including bin files) uploaded at NVC can be replicated to CCD to allow posts to view this supporting documentation. In addition, eDP Web interfaces with CCD to allow a subset of CCD users to view eDP data. This subset of CCD users are those CCD users who have been given access to the IV/DV (Diversity Visa) Applicant Full and IV/DV Applicant Summary reports on CCD.

Immigrant Visa Information System (IVIS) – Views of IVIS data are used to associate the eDP data to the IVIS case/applicant; IVIS is also used by eDP to identify the type of eDP user by their role. See the matrix of eDP user roles below.

Role	Search Case	Scan Docs/ Batch Scan	Attach Docs	Manage Docs						View Docs	Print Bar-codes	Bin Files			Process Images
				Edit PDF Doc.	Compress Docs	Delete Docs	Restore Docs	Edit Doc Details	Drag and Drop Files			Search	Attach New	View	
eDP Manager	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
eDP Data Entry	✓	✓	✓	✓	✓	X	✓	✓	✓	✓	✓	✓	✓	✓	✓
eDP Read Only	✓	X	X	X	X	X	✓	X	✓	✓	X	✓	X	✓	X

Immigrant Visa Overseas (IVO) – receives bin file data from eDP by way of CCD when IVO shadow tables are populated by bin files from CCD.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

Information is shared by secure transmission methods permitted by internal Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. Security Officers determine the access level an application user (including managers) may require depending on the user's particular job function and level of clearance. System managers and business owners are responsible for safeguarding the records processed, stored, or transmitted by eDP and eDP Web. Access to electronic

files is protected by passwords, and is under the supervision of system managers. Audit trails track and monitor usage and access. Finally, regularly administered security/privacy training informs authorized users of proper handling procedures.

An Interface Control Document (ICD) is used to define and disclose transmission formats via OpenNet. The Department of State systems that interface with eDP/eDP Web are strictly controlled by Firewall and Network Intrusion Detection System (NIDS) rules sets that limit ingress and egress to them. All changes are requested from the Firewall Advisory Board (FAB) using a Universal Trouble Ticket (UTT). Each UTT is vetted by technical personnel and management prior to the change being implemented.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

The risks associated with sharing privacy information internally and the disclosure of privacy information is generally associated with personnel. Intentional and unintentional disclosure of privacy information from personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. To combat the misuse of information by personnel, numerous management, operational and technical controls are in place to reduce and mitigate the risks associated with internal sharing and disclosure including, but not limited to, annual security training, separation of duties, least privilege and personnel screening. Management Control Reports identify actions of authorized users and allow management to review daily activity. User training at the application level is delivered annually in accordance with internal Department of State regulations.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

eDP does not directly share information with external organizations, although eDP Web users do include CCD users from external agencies such as DHS. This external sharing arrangement is detailed in the CCD PIA.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

eDP and eDP Web do not directly share information with external organizations.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

eDP and eDP Web do not directly share information with external organizations.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

Visa Records, State-39

☐ does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Neither eDP nor eDP Web are public facing systems so any notice regarding submission of immigrant visa forms and supporting documentation are provided earlier in the submission process on the forms identified in section 3(b) herein and attachments thereto.

The application forms provide a statement that the information collected is protected by section 222(f) of INA. INA section 222(f) provides that visa issuance and refusal records shall be considered confidential and shall be used only for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States. Certified copies of visa records may be made available to a court which certifies that the information contained in such records is needed in a case pending before the court.

eDP is an internal application used by NVC. The IV applicant, petitioner or legal representative provides paper and electronic copies of documents to be attached to the applicant's immigrant visa records, but has no direct access to the client workstations on which eDP is installed. eDP Web is not used to collect information from users.

b. Do individuals have the opportunity and/or right to decline to provide information?

eDP and eDP Web are not public facing systems. However, IV applicants, petitioners or legal representatives have the right to decline to provide PII for use in processing their immigration visa application, but failure to provide the information necessary to process the application may result in the application being rejected.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

eDP and eDP Web are not public facing systems. Information is given voluntarily by the applicants or their representatives for the purpose of obtaining an immigrant visa. No other special uses of the information are permitted. Individuals are advised on the use of the information being collected at the time of collection.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

eDP and eDP Web rely on State-39 and on the notice given to the petitioners who complete immigrant visa records that reside in eDP and eDP Web to mitigate the privacy risks posed by collection and use of PII.

The mechanisms for notice offered to individuals are reasonable and adequate in relation to the system's purpose and uses. The information provided by the applicant is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA). The information provided on the forms and in

the System of Records Notice (SORN) regarding visa records fully explain how the information may be used by the Department and how it is protected.

Access to eDP and eDP Web is restricted to cleared, authorized Department of State direct hires and contractor personnel and cleared CCD users. eDP and eDP Web enforce the concept of least privilege by ensuring that users are restricted to only those functions which are required to perform their assigned duties.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

eDP and eDP Web are not public facing systems. IV applicants may change their information at any time prior to submission of the application. Once that is done, applicants may make changes only by filing a new application with the Department or correcting the information during the course of a visa interview. The Department will release the following information to a visa applicant upon request, and this guidance is available to the public in 9 FAM 40.4:

(1) Correspondence previously sent to or given to the applicant by the post;

(2) Civil documents presented by the applicant and

(3) Visa applications and any other documents, including sworn statements, submitted by the applicant to the consular officer in the form in which they were submitted, i.e., with any remarks or notations by U.S. Government employees deleted.

Information in eDP and eDP Web is considered part of a visa record subject to confidentiality requirements under INA 222(f). eDP and eDP Web information may also be protected in accordance with provisions of the Privacy Act of 1974 (5 U.S.C. 552a). In addition, covered petitioners may request access to or correction of their PII pursuant to FOIA or the Privacy Act, as appropriate.

Procedures for notification and redress are published in the Privacy Act SORN, and in rules published at 22 CFR 171.31 informing the individual regarding how to inquire about the existence of records, how to request access to the records, and how to request amendment of a record. Certain exemptions to Privacy Act provisions for notification and redress may exist for visa records on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.32.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

To the extent scanned information in eDP and eDP Web may be covered under the Privacy Act, the notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the immigrant visa process. Therefore privacy risks associated with notification and redress are appropriately addressed at the time that the petitioner submits the immigrant visa application.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Internal access to eDP and eDP Web is limited to authorized Department of State users, including cleared contractors, who have a justified need for the information in order to perform official duties. To access the system, users must be granted the status of an authorized user of the Department of State's unclassified network. Each authorized user must sign a user access agreement before being given a user account. The authorized user's supervisor must sign the agreement certifying that access is needed to perform official duties. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). Completed applications are also reviewed and approved by the Information System Security Officer (ISSO) prior to assigning a logon. The level of access for the authorized user restricts the data that may be viewed and the degree to which data may be modified. A system use notification ("warning banner") is displayed before logon is permitted and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

User access to information immigrant visa applications is restricted according to job responsibilities and requires managerial level approvals. Access control lists permit categories of information and reports that are to be restricted. Security Officers determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance. The Operations Unit at NVC serves as the administrator for creating and modifying IVIS accounts, granting the appropriate level of system access based on the determination of the unit manager. Mandatory annual security/privacy training is required for all authorized users including security training and regular refreshment training.

Specific to eDP Web users' access via CCD:
Access to CCD requires a unique user account and password. Each domestic organization appoints a Certifying Authority who is responsible for reviewing each CCD user account request and creating the CCD user account. The Certifying Authority is also responsible for periodically reviewing the user access list and disabling any user account that no longer requires access. eDP Web user accounts are restricted to those CCD users who have been given access by the Certifying Authority to the IV/DV Applicant Full report and the IV/DV Applicant Summary report on CCD. DV refers to diversity visa.

The CCD access for post users is controlled by Consular Shared Tables (CST) roles granted and managed by CST administrators. Each post has a CST administrator responsible for accepting, reviewing, and creating the individual user accounts.

Once a user is properly identified and authenticated by the CCD, they are authorized to perform all functions commensurate with their CCD assigned role. The CCD employs logical access controls in accordance with the principle of least privilege and the concept of separation of duties.

Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly deleted. Additionally, system audit trails are regularly analyzed and reviewed to deter and detect any

unauthorized activity. (An audit trail provides a record of all functions that authorized users perform--or may attempt to perform.)

b. What privacy orientation or training for the system is provided authorized users?

All users must pass computer security and privacy awareness training prior to receiving access to the system and must complete annual refresher training to retain access. Additionally, all Department employees must pass the PA-459 course, entitled Protecting Personally Identifiable Information.

Department of State users must read and accept the Computer Fraud and Abuse Act Notice and Privacy Act Notice that outline the expected use of these systems and how they are subject to monitoring prior to being granted access.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Access control lists, which define who can access the eDP and eDP Web systems, and at what privilege level, are regularly reviewed. Inactive accounts are promptly archived. Additionally, system audit trails are regularly analyzed and reviewed to deter and detect any unauthorized activity. Audit trails provide a record of all functions authorized users perform or may attempt to perform.

11. Technologies

a. What technologies are used in the system that involve privacy risk?

eDP and eDP Web operate under standard, commercially-available software products residing on a government-operated computing platforms not shared by other business applications or technologies. eDP and eDP Web do not employ any technology known to elevate privacy risk.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

Since eDP does not use any technology known to elevate privacy risk, standard robust safeguards are determined to be satisfactory in this application.

12. Security

a. What is the security certification and accreditation (C&A) status of the system?

The Department of State will operate eDP and eDP Web in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately safeguarded and protected. The Department of State is in the process of conducting a risk assessment of the system to identify appropriate security controls to protect against risk. The Department of State performs routine monitoring, testing, and evaluation of security controls to ensure that the controls continue to fully function.

These are new systems that are undergoing their first C&A process. Once an ATO is achieved, any significant change to eDP or eDP Web will be reviewed by the CA ISSO security specialists. In accordance with the Federal Information Security Management Act (FISMA) provisions, as new systems, eDP and eDP Web are on schedule to complete their initial Certification and Accreditation (C&A) with a projected completion by August 2012.